

What is claimed is:

1 1. A digital work protection system including a recording  
2 apparatus and a plurality of reproduction apparatuses, the  
3 recording apparatus being operable to encrypt a content and write  
4 the encrypted content onto a recording medium, and the plurality  
5 of reproduction apparatuses each being operable to attempt to  
6 decrypt the encrypted content recorded on the recording medium,  
7 wherein

8 one or more of the plurality of reproduction apparatuses  
9 are revoked,

10 the recording medium has (i) a read-only unrewritable  
11 area in which a medium inherent number inherent to the recording  
12 medium is prestored and (ii) a rewritable area to and from which  
13 data can be written and read, and

14 the recording apparatus includes:

15 a storing unit that stores therein a piece of media  
16 key data including a plurality of encrypted media keys generated  
17 by (i) for each of unrevoked reproduction apparatuses, encrypting  
18 a media key using a device key of the unrevoked reproduction  
19 apparatus respectively, and (ii) for each of the revoked  
20 reproduction apparatuses, encrypting predetermined detection  
21 information using a device key of the revoked reproduction  
22 apparatus respectively;

23                   a reading unit operable to read the medium inherent  
24   number from the unrewritable area of the recording medium;

25                   a generating unit operable to generate an  
26   encryption key based on the read medium inherent number and the  
27   media key;

28                   an encrypting unit operable to encrypt the content  
29   being a piece of digital data, based on the generated encryption  
30   key, so as to generate the encrypted content;

31                   a reading unit operable to read the piece of media  
32   key data from the storing unit; and

33                   a writing unit operable to write the read piece  
34   of media key data and the generated encrypted content into the  
35   rewritable area of the recording medium, and

36           each of the reproduction apparatuses includes:

37                   a reading unit operable to read one encrypted media  
38   key that corresponds to the reproduction apparatus, from the  
39   piece of media key data recorded in the rewritable area of the  
40   recording medium;

41                   a decrypting unit operable to decrypt the read  
42   encrypted media key using the device key of the reproduction  
43   apparatus, so as to generate a decryption media key;

44                   a controlling unit operable to judge whether the  
45   generated decryption media key is the detection information or  
46   not, to prohibit the encrypted content from being decrypted when

47 having judged in the affirmative, and to permit the encrypted  
48 content to be decrypted when having judged in the negative; and  
49 a decrypting unit operable to, when the encrypted  
50 content is permitted to be decrypted, read the encrypted content  
51 from the recording medium and decrypt the read encrypted content  
52 based on the generated decryption media key, so as to generate  
53 a decrypted content.

1 2. A recording apparatus that is operable to encrypt a content  
2 and write the encrypted content onto a first recording medium  
3 and is used in a digital work protection system which includes  
4 the recording apparatus and a plurality of reproduction  
5 apparatuses each being operable to attempt to decrypt the  
6 encrypted content recorded on the first recording medium, wherein  
7 one or more of the plurality of reproduction apparatuses  
8 are revoked,  
9 the first recording medium has (i) a read-only  
10 unrewritable area in which a medium inherent number inherent  
11 to the first recording medium is prestored and (ii) a rewritable  
12 area to and from which data can be written and read, and  
13 the recording apparatus includes:  
14 a storing unit that stores therein a first piece  
15 of media key data including a plurality of encrypted media keys  
16 generated by (i) for each of unrevoked reproduction apparatuses,

17 encrypting a media key using a device key of the unrevoked  
18 reproduction apparatus respectively, and (ii) for each of the  
19 revoked reproduction apparatuses, encrypting predetermined  
20 detection information using a device key of the revoked  
21 reproduction apparatus respectively;

22                   a first reading unit operable to read the medium  
23 inherent number from the unrewritable area;

24                   a generating unit operable to generate an encryption  
25 key based on the read medium inherent number and the media key;

26                   an encrypting unit operable to encrypt the content  
27 being a piece of digital data, based on the generated encryption  
28 key, so as to generate the encrypted content;

29                   a second reading unit operable to read the first  
30 piece of media key data from the storing unit; and

31                   a writing unit operable to write the read first piece  
32 of media key data and the generated encrypted content into the  
33 rewritable area.

1    3.       The recording apparatus of Claim 2, wherein

2                   a second recording medium stores therein a second piece  
3 of media key data including another set of encrypted media keys  
4 generated by (i) for each of unrevoked reproduction apparatuses,  
5 encrypting the media key using a device key of the unrevoked  
6 reproduction apparatus respectively, and (ii) for each of revoked

7 reproduction apparatuses, encrypting predetermined detection  
8 information using a device key of the revoked reproduction  
9 apparatus respectively, and  
10 the recording apparatus further includes:  
11 a comparing unit operable to compare the second  
12 piece of media key data recorded on the second recording medium  
13 with the first piece of media key data stored in the storing  
14 unit so as to judge which is newer; and  
15 an updating unit operable to, when the second piece  
16 of media key data has been judged newer, read the second piece  
17 of media key data from the second recording medium and overwrite  
18 the first piece of media key data stored in the storing unit  
19 with the second piece of media key data, and  
20 the second reading unit reads the second piece of media  
21 key data from the storing unit, instead of the first piece of  
22 media key data, and  
23 the writing unit writes the second piece of media key  
24 data, instead of the first piece of media key data, into the  
25 rewritable area.

1 4. The recording apparatus of Claim 3, wherein  
2 the first piece of media key data stored in the storing  
3 unit includes a first piece of version information indicating  
4 a generation of the first piece of media key data,

5           the second piece of media key data recorded on the second  
6   recording medium includes a second piece of version information  
7   indicating a generation of the second piece of media key data,  
8   and

9           the comparing unit judges which one of the first piece  
10   of media key data and the second piece of media key data is newer  
11   by comparing the first piece of version information with the  
12   second piece of version information.

1   5.       The recording apparatus of Claim 3, wherein  
2           the first piece of media key data stored in the storing  
3   unit includes a first piece of date and time information  
4   indicating a date and time at which the first piece of media  
5   key data has been generated,

6           the second piece of media key data recorded on the second  
7   recording medium includes a second piece of data and time  
8   information indicating a date and time at which the second piece  
9   of media key data has been generated, and

10          the comparing unit judges which one of the first piece  
11   of media key data and the second piece of media key data is newer  
12   by comparing the first piece of date and time information with  
13   the second piece of date and time information.

1   6.       The recording apparatus of Claim 2, wherein

2           the storing unit further stores therein a piece of  
3   revocation data indicating one or more of public keys assigned  
4   to the recording apparatus and the plurality of reproduction  
5   apparatuses are revoked,

6           the recording apparatus further includes a signature  
7   generating unit operable to use a digital signature function  
8   on the piece of revocation data, so as to generate a piece of  
9   verification information, and

10          the writing unit further writes the generated piece of  
11   verification information into the rewritable area of the first  
12   recording medium.

1   7.       The recording apparatus of Claim 6, wherein

2           the signature generating unit uses a digital signature  
3   with appendix on the piece of revocation data to generate a piece  
4   of signature data, so as to generate the piece of verification  
5   information from the generated piece of signature data and the  
6   piece of revocation data, and

7           the writing unit writes the piece of verification  
8   information.

1   8.       The recording apparatus of Claim 6, wherein

2           the signature generating unit uses a digital signature  
3   with message recovery on the piece of revocation data to generate

4 the piece of verification information.

1 9. The recording apparatus of Claim 6, wherein  
2 the storing unit further stores therein a secret key and  
3 a public key certificate of the recording apparatus,  
4 the signature generating unit uses the digital signature  
5 function using the stored secret key,  
6 the second reading unit further reads the public key  
7 certificate from the storing unit, and  
8 the writing unit writes the read public key certificate  
9 into the rewritable area of the first recording medium.

1 10. The recording apparatus of Claim 2, wherein  
2 the storing unit further stores therein a public key  
3 certificate of the recording apparatus,  
4 the second reading unit reads the public key certificate  
5 from the storing unit, and  
6 the writing unit writes the read public key certificate  
7 into the rewritable area of the first recording medium.

1 11. The recording apparatus of Claim 2, wherein  
2 the storing unit further stores therein a piece of  
3 revocation data indicating one or more of public keys assigned  
4 to the recording apparatus and the plurality of reproduction



5     apparatuses are revoked,

6             the recording apparatus further includes a signature  
7     generating unit operable to use a digital signature function  
8     on the piece of revocation data so as to generate a piece of  
9     verification information, and

10            the writing unit further writes the generated piece of  
11     verification information onto the second recording medium.

1     12.     The recording apparatus of Claim 2, wherein

2             the storing unit further stores therein a piece of  
3     revocation data indicating one or more of public keys assigned  
4     to the recording apparatus and the plurality of reproduction  
5     apparatuses are revoked,

6             the second reading unit further reads the piece of  
7     revocation data from the storing unit, and

8             the writing unit writes the read piece of revocation data  
9     onto the second recording medium.

1     13.     The recording apparatus of Claim 2, wherein

2             the storing unit further stores therein a public key  
3     certificate of the recording apparatus,

4             the second reading unit further reads the public key  
5     certificate from the storing unit, and

6             the writing unit writes the read public key certificate

7 onto the second recording medium.

1 14. The recording apparatus of Claim 2, wherein  
2 the storing unit further stores therein an apparatus  
3 identifier that identifies the recording apparatus,  
4 the recording apparatus further includes an embedding  
5 unit operable to read the apparatus identifier and embed the  
6 read apparatus identifier into the content as an electronic  
7 watermark, and  
8 the encrypting unit encrypts the content into which the  
9 apparatus identifier is embedded.

1 15. The recording apparatus of Claim 2, wherein  
2 the first piece of media key data stored in the storing  
3 unit further includes a first data identifier that identifies  
4 the first piece of media key data,  
5 the writing unit (i) writes the first data identifier  
6 and the encrypted content into the rewritable area of the first  
7 recording medium in such a manner that the first data identifier  
8 and the encrypted content are in correspondence with each other,  
9 and (ii) writes the first piece of media key data including the  
10 first data identifier into the rewritable area.

1 16. The recording apparatus of Claim 15, wherein

2           the first recording medium further stores therein a second  
3 piece of media key data including another set of encrypted media  
4 keys generated by (i) for each of unrevoked reproduction  
5 apparatuses, encrypting a media key using a device key of the  
6 unrevoked reproduction apparatus respectively, and (ii) for each  
7 of revoked reproduction apparatuses, encrypting predetermined  
8 detection information using a device key of the revoked  
9 reproduction apparatus respectively,

10           the second piece of media key data includes a second data  
11 identifier that identifies the second piece of media key data,  
12 and

13           the recording apparatus further includes an assigning  
14 unit operable to assign the first data identifier, which is  
15 different from the second data identifier, to the first piece  
16 of media key data stored in the storing unit.

1 17.       The recording apparatus of Claim 15, further including:

2           a comparing unit operable to compare the first piece of  
3 media key data stored in the storing unit with a second piece  
4 of media key data recorded on the second recording medium so  
5 as to judge which is newer; and

6           an assigning unit operable to assign the first data  
7 identifier to the first piece of media key data when the first  
8 piece of media key data has been judged newer.

1 18. The recording apparatus of Claim 17, wherein  
2 the first piece of media key data stored in the storing  
3 unit includes a first piece of date and time information  
4 indicating a date and time at which the first piece of media  
5 key data has been generated,  
6 a second piece of media key data stored in the first  
7 recording medium includes a second piece of data and time  
8 information indicating a date and time at which the second piece  
9 of media key data has been generated, and  
10 the comparing unit judges which one of the first piece  
11 of media key data and the second piece of media key data is newer  
12 by comparing the first piece of date and time information with  
13 the second piece of date and time information.

1 19. A reproduction apparatus included in a digital work  
2 protection system made up of at least a plurality of reproduction  
3 apparatuses and a recording apparatus operable to encrypt a  
4 content and write the encrypted content onto a first recording  
5 medium, the plurality of reproduction apparatuses each being  
6 operable to attempt to decrypt the encrypted content recorded  
7 on the first recording medium; wherein  
8 one or more of the plurality of reproduction apparatuses  
9 are revoked,  
10 the first recording medium has (i) a read-only

11 unrewritable area in which a medium inherent number inherent  
12 to the first recording medium is prestored and (ii) a rewritable  
13 area to and from which data can be written and read,

14 the recording apparatus stores therein a piece of media  
15 key data including a plurality of encrypted media keys generated  
16 by (i) for each of unrevoked reproduction apparatuses, encrypting  
17 a media key using a device key of the unrevoked reproduction  
18 apparatus respectively, and (ii) for each of the revoked  
19 reproduction apparatuses, encrypting predetermined detection  
20 information using a device key of the revoked reproduction  
21 apparatus respectively,

22 the recording apparatus (i) reads the medium inherent  
23 number from the unrewritable area of the first recording medium  
24 (ii) generates an encryption key based on the read medium-inherent  
25 number and the media key, (iii) encrypts the content being a  
26 piece of digital data based on the generated encryption key to  
27 generate the encrypted content, (iv) reads the piece of media  
28 key data from the storing unit, and (v) writes the read piece  
29 of media key data and the generated encrypted content into the  
30 rewritable area of the first recording medium, and

31 the reproduction apparatus includes:

32 a reading unit operable to read one encrypted media  
33 key that corresponds to the reproduction apparatus, from the  
34 piece of media key data recorded in the rewritable area;

35                   a first decrypting unit operable to decrypt the  
36 read encrypted media key using the device key of the reproduction  
37 apparatus, so as to generate a decryption media key;

38                   a controlling unit operable to judge whether the  
39 generated decryption media key is the detection information or  
40 not, to prohibit the encrypted content from being decrypted when  
41 having judged in the affirmative, and to permit the encrypted  
42 content to be decrypted when having judged in the negative; and

43                   a second decrypting unit operable to, when the  
44 encrypted content is permitted to be decrypted, read the  
45 encrypted content from the first recording medium and decrypt  
46 the read encrypted content based on the generated decryption  
47 media key, so as to generate a decrypted content.

1   20.     The reproduction apparatus of Claim 19, wherein  
2           the recording apparatus further stores therein a piece  
3 of revocation data indicating one or more of public keys assigned  
4 to the recording apparatus and the plurality of reproduction  
5 apparatuses are revoked, uses a digital signature function on  
6 the piece of revocation data to generate a piece of verification  
7 information, and writes the generated piece of verification  
8 information into the rewritable area of the first recording  
9 medium,  
10          the reading unit further reads the piece of verification

11 information recorded in the rewritable area,  
12 the reproduction apparatus further includes a verifying  
13 unit operable to implement signature verification based on the  
14 read piece of verification information and output a verification  
15 result indicating either a verification success or a verification  
16 failure, and

17 the controlling unit further prohibits the encrypted  
18 content from being decrypted when the verification result  
19 indicates a verification failure, and permits the encrypted  
20 content to be decrypted when the verification result indicates  
21 a verification success.

1 21. The reproduction apparatus of Claim 20, wherein  
2 the recording apparatus (i) uses a digital signature with  
3 appendix on the piece of revocation data to generate a piece  
4 of signature data, (ii) generates the piece of verification  
5 information from the generated piece of signature data and the  
6 piece of revocation data, (iii) writes the generated piece of  
7 verification information, and  
8 the verifying unit implements the signature verification  
9 based on the piece of signature data included in the piece of  
10 verification information.

1 22. The reproduction apparatus of Claim 20, wherein

2           the recording apparatus uses a digital signature with  
3 message recovery on the piece of revocation data to generate  
4 the piece of verification information, and  
5           the verifying unit generates, when the verification  
6 result indicates a verification success, the piece of revocation  
7 data from the piece of verification information.

1 23.     The reproduction apparatus of Claim 20, wherein  
2           the recording apparatus further stores therein a secret  
3 key and a public key certificate of the recording apparatus,  
4           the recording apparatus (i) uses the digital signature  
5 function using the stored secret key, (ii) reads the public key  
6 certificate, and (iii) writes the read public key certificate  
7 into the rewritable area of the first recording medium, and  
8           the verifying unit reads the public key certificate from  
9 the first recording medium, extracts a public key from the read  
10 public key certificate, and implements the signature  
11 verification using the extracted public key.

1 24.     The reproduction apparatus of Claim 20, wherein  
2           the recording apparatus stores therein the piece of  
3 revocation data, uses a digital signature function on the piece  
4 of revocation data to further generate another piece of  
5 verification information, and writes the generated piece of



6 verification information onto a second recording medium,  
7 the reading unit reads the other piece of verification  
8 information from the second recording medium instead of from  
9 the first recording medium, and  
10 the verifying unit implements the signature verification  
11 based on the other piece of verification information read from  
12 the second recording medium.

1 25. The reproduction apparatus of Claim 19, wherein  
2 the recording apparatus further stores therein a public  
3 key certificate of the recording apparatus, reads the public  
4 key certificate, and writes the read public key certificate into  
5 the rewritable area of the first recording medium,  
6 the reproduction apparatus further includes:  
7 a storing unit that stores therein a first piece  
8 of revocation data indicating one or more of public keys assigned  
9 to the recording apparatus and the plurality of reproduction  
10 apparatuses are revoked;  
11 a certificate reading unit operable to read the  
12 public key certificate from the first recording medium; and  
13 a public key verifying unit operable to check  
14 whether a public key included in the read public key certificate  
15 is revoked according to the first piece of verification data,  
16 and

17           the controlling unit further prohibits the encrypted  
18 content from being decrypted when the public key is revoked,  
19 and permits the encrypted content to be decrypted when the public  
20 key is not revoked.

1    26.   The reproduction apparatus of Claim 25, wherein  
2           a second recording medium stores therein a second piece  
3 of revocation data indicating one or more of public keys assigned  
4 to the recording apparatus and the plurality of reproduction  
5 apparatuses are revoked,  
6           the reproduction apparatus further includes:  
7                 a comparing unit operable to compare the second  
8 piece of revocation data recorded on the second recording medium  
9 with the first piece of revocation data stored in the storing  
10 unit so as to judge which is newer; and  
11            an updating unit operable to, when the second piece  
12 of revocation data has been judged newer, read the second piece  
13 of revocation data from the second recording medium and overwrite  
14 the first piece of revocation data in the storing unit with the  
15 read second piece of revocation data.

1    27.   The reproduction apparatus of Claim 26, wherein  
2           the comparing unit judges which one of the first piece  
3 of revocation data and the second piece of revocation data is

4 newer by comparing sizes of the first and second pieces of  
5 revocation data.

1 28. The reproduction apparatus of Claim 26, wherein  
2 the comparing unit judges which one of the first piece  
3 of revocation data and the second piece of revocation data is  
4 newer by comparing numbers of the revoked public keys indicated  
5 by the first and second pieces of revocation data.

1 29. The reproduction apparatus of Claim 26, wherein  
2 the first piece of revocation data stored in the storing  
3 unit includes a first piece of version information indicating  
4 a generation of the first piece of revocation data,  
5 the second piece of revocation data recorded on the second  
6 recording medium includes a second piece of version information  
7 indicating a generating of the second piece of revocation data,  
8 and  
9 the comparing unit judges which one of the first piece  
10 of revocation data and the second piece of revocation data is  
11 newer by comparing the first and second pieces of version  
12 information.

1 30. The reproduction apparatus of Claim 26, wherein  
2 the first piece of revocation data stored in the storing

3 unit includes a first piece of date and time information  
4 indicating a date and time at which the first piece of revocation  
5 data has been generated,  
6 the second piece of revocation data recorded on the second  
7 recording medium includes a second piece of date and time  
8 information indicating a date and time at which the second piece  
9 of revocation data has been generated, and  
10 the comparing unit judges which one of the first piece  
11 of revocation data and the second piece of revocation data is  
12 newer by comparing the first and second pieces of date and time  
13 information.

1 31. The reproduction apparatus of Claim 25, wherein  
2 the recording apparatus further stores therein a second  
3 piece of revocation data indicating one or more of public keys  
4 assigned to the recording apparatus and the plurality of  
5 reproduction apparatuses are revoked,  
6 the recording apparatus reads the second piece of  
7 revocation data and writes the read second piece of revocation  
8 data onto a second recording medium, and  
9 the public key verifying unit reads the second piece of  
10 revocation data, instead of the first piece of revocation data,  
11 from the second recording medium, and verifies if the public  
12 key is revoked according to the second piece of revocation data.

1 32. The reproduction apparatus of Claim 25, wherein  
2 the recording apparatus further stores therein a public  
3 key certificate of the recording apparatus,  
4 the recording apparatus reads the public key certificate  
5 and writes the read public key certificate onto a second recording  
6 medium, and  
7 the certificate reading unit reads the public key  
8 certificate from the second recording medium instead of from  
9 the first recording medium.

1 33. The reproduction apparatus of Claim 19, further  
2 comprising:  
3 a storing unit that stores therein an apparatus identifier  
4 that identifies the reproduction apparatus; and  
5 an embedding unit operable to, when the encrypted content  
6 is permitted to be decrypted, read the apparatus identifier from  
7 the storing unit and embed the read apparatus identifier into  
8 the encrypted content as an electronic watermark, and  
9 a writing unit operable to write the encrypted content  
10 in which the apparatus identifier is embedded onto the first  
11 recording medium.

1 34. The reproduction apparatus of Claim 19, wherein  
2 the piece of media key data stored in the recording

3 apparatus further includes a data identifier that identifies  
4 the piece of media key data,  
5 the recording apparatus writes the data identifier and  
6 the encrypted content into the rewritable area in such a manner  
7 that the data identifier and the encrypted content are in  
8 correspondence with each other, and writes the piece of media  
9 key data including the data identifier into the rewritable area,  
10 and  
11 the reproduction apparatus further includes:  
12 a receiving unit operable to receive a specification  
13 of the encrypted content recorded on the first recording medium;  
14 a first reading unit operable to read, from the first  
15 recording medium, the data identifier that is in correspondence  
16 with the encrypted content in the received specification; and  
17 a second reading unit operable to read the piece  
18 of media key data including the data identifier from the first  
19 recording medium, and  
20 the controlling unit judges whether the encrypted content  
21 is prohibited from being decrypted or permitted to be decrypted  
22 based on the read piece of media key data.

1 35. A recording method used by a recording apparatus that  
2 is operable to encrypt a content and write the encrypted content  
3 onto a recording medium and is included in a digital work

4 protection system being made up of at least the recording  
5 apparatus and a plurality of reproduction apparatuses each being  
6 operable to attempt to decrypted the encrypted content, wherein  
7 one or more of the plurality of reproduction apparatuses  
8 are revoked,  
9 the recording medium has (i) a read-only unrewritable  
10 area in which a medium inherent number inherent to the recording  
11 medium is prestored and (ii) a rewritable area to and from which  
12 data can be written and read, and  
13 the recording apparatus includes  
14 a storing unit that stores therein a piece of  
15 media key data including a plurality of encrypted media keys  
16 generated by (i) for each of unrevoked reproduction apparatuses,  
17 encrypting a media key using a device key of the unrevoked  
18 reproduction apparatus respectively, and (ii) for each of the  
19 revoked reproduction apparatuses, encrypting predetermined  
20 detection information using a device key of the revoked  
21 reproduction apparatus respectively, and  
22 the recording method includes:  
23 a first reading step of reading the medium inherent  
24 number from the unrewritable area of the recording medium;  
25 a generating step of generating an encryption key  
26 based on the read medium inherent number and the media key;  
27 an encrypting step of encrypting the content being

28 a piece of digital data, based on the generated encryption key,  
29 so as to generate the encrypted content;  
30 a second reading step of reading the piece of media  
31 key data from the storing unit; and  
32 a writing step of writing the read piece of media  
33 key data and the generated encrypted content into the rewritable  
34 area of the recording medium.

1 36. A recording-purpose computer program to be used by a  
2 recording apparatus that is operable to encrypt a content and  
3 write the encrypted content onto a recording medium and is  
4 included in a digital work protection system being made up of  
5 at least the recording apparatus and a plurality of reproduction  
6 apparatuses each being operable to attempt to decrypt the  
7 encrypted content, wherein

8 one or more of the plurality of reproduction apparatuses  
9 are revoked,

10 the recording medium has (i) a read-only unrewritable  
11 area in which a medium inherent number inherent to the recording  
12 medium is prestored and (ii) a rewritable area to and from which  
13 data can be written and read, and

14 the recording apparatus includes

15 a storing unit that stores therein a piece of media  
16 key data including a plurality of encrypted media keys generated



17 by (i) for each of unrevoked reproduction apparatuses, encrypting  
18 a media key using a device key of the unrevoked reproduction  
19 apparatus respectively, and (ii) for each of the revoked  
20 reproduction apparatuses, encrypting predetermined detection  
21 information using a device key of the revoked reproduction  
22 apparatus respectively, and

23 the recording-purpose computer program includes:

24 a first reading step of reading the medium inherent  
25 number from the unrewritable area of the recording medium;

26 a generating step of generating an encryption key  
27 based on the read medium inherent number and the media key;

28 an encrypting step of encrypting the content being  
29 a piece of digital data, based on the generated encryption key,  
30 so as to generate the encrypted content;

31 a second reading step of reading the piece of media  
32 key data from the storing unit; and

33 a writing step of writing the read piece of media  
34 key data and the generated encrypted content into the rewritable  
35 area of the recording medium.

1 37. The recording-purpose computer program of Claim 36, being  
2 recorded on a computer-readable recording medium.

1 38. A reproduction method to be used by each of reproduction

2 apparatuses included in a digital work protection system made  
3 up of at least the reproduction apparatuses and a recording  
4 apparatus operable to encrypt a content and write the encrypted  
5 content onto a recording medium, the reproduction apparatuses  
6 each being operable to attempt to decrypt the encrypted content,  
7 wherein

8 one or more of the plurality of reproduction apparatuses  
9 are revoked,

10 the recording medium has (i) a read-only unrewritable  
11 area in which a medium inherent number inherent to the recording  
12 medium is prestored and (ii) a rewritable area to and from which  
13 data can be written and read, and

14 the recording apparatus stores therein a piece of media  
15 key data including a plurality of encrypted media keys generated  
16 by (i) for each of unrevoked reproduction apparatuses, encrypting  
17 a media key using a device key of the unrevoked reproduction  
18 apparatus respectively, and (ii) for each of the revoked  
19 reproduction apparatuses, encrypting predetermined detection  
20 information using a device key of the revoked reproduction  
21 apparatus respectively,

22 the recording apparatus (i) reads the medium inherent  
23 number from the unrewritable area of the recording medium, (ii)  
24 generates an encryption key based on the read medium inherent  
25 number and the media key, (iii) encrypts the content being a

26 piece of digital data based on the generated encryption key to  
27 generate the encrypted content, (v) reads the piece of media  
28 key data from the storing unit, and (vi) writes the read piece  
29 of media key data and the generated encrypted content into the  
30 rewritable area of the recording medium, and

31 the reproduction method includes:

32 a reading step of reading one encrypted media key  
33 that corresponds to the reproduction apparatus, from the piece  
34 of media key data recorded in the rewritable area of the recording  
35 medium;

36 a first decrypting step of decrypting the read  
37 encrypted media key using the device key of the reproduction  
38 apparatus, so as to generate a decryption media key;

39 a controlling step of judging whether the  
40 generated decryption media key is the detection information or  
41 not, prohibiting the encrypted content from being decrypted when  
42 having judged in the affirmative, and permitting the encrypted  
43 content to be decrypted when having judged in the negative; and

44 a second decrypting step of, when the encrypted  
45 content is permitted to be decrypted, reading the encrypted  
46 content from the recording medium, and decrypting the read  
47 encrypted content based on the generated decryption media key,  
48 so as to generate a decrypted content.

1 39. A reproduction-purpose computer program to be used by  
2 each of reproduction apparatuses that are included in a digital  
3 work protection system made up of at least the reproduction  
4 apparatuses and a recording apparatus being operable to encrypt  
5 a content and write the encrypted content onto a recording medium,  
6 the reproduction apparatuses each being operable to decrypt the  
7 encrypted content, wherein  
8 one or more of the plurality of reproduction apparatuses  
9 are revoked,  
10 the recording medium has (i) a read-only unrewritable  
11 area in which a medium inherent number inherent to the recording  
12 medium is prestored and (ii) a rewritable area to and from which  
13 data can be written and read, and  
14 the recording apparatus stores therein a piece of media  
15 key data including a plurality of encrypted media keys generated  
16 by (i) for each of unrevoked reproduction apparatuses, encrypting  
17 a media key using a device key of the unrevoked reproduction  
18 apparatus respectively, and (ii) for each of the revoked  
19 reproduction apparatuses, encrypting predetermined detection  
20 information using a device key of the revoked reproduction  
21 apparatus respectively,  
22 the recording apparatus (i) reads the medium inherent  
23 number from the unrewritable area of the recording medium, (ii)  
24 generates an encryption key based on the read medium inherent

25 number and the media key, (iii) encrypts the content being a  
26 piece of digital data based on the generated encryption key to  
27 generate the encrypted content, (v) reads the piece of media  
28 key data from the storing unit, and (vi) writes the read piece  
29 of media key data and the generated encrypted content into the  
30 rewritable area of the recording medium, and

31 the reproduction-purpose computer program includes:

32 a reading step of reading one encrypted media key  
33 that corresponds to the reproduction apparatus, from the piece  
34 of media key data recorded in the rewritable area of the recording  
35 medium;

36 a first decrypting step of decrypting the read  
37 encrypted media key using the device key of the reproduction  
38 apparatus, so as to generate a decryption media key;

39 a controlling step of judging whether the  
40 generated decryption media key is the detection information or  
41 not, prohibiting the encrypted content from being decrypted when  
42 having judged in the affirmative, and permitting the encrypted  
43 content to be decrypted when having judged in the negative; and

44 a second decrypting step of, when the encrypted  
45 content is permitted to be decrypted, reading the encrypted  
46 content from the recording medium, and decrypting the read  
47 encrypted content based on the generated decryption media key,  
48 so as to generate a decrypted content.

1 40. The reproduction-purpose computer program of Claim 39,  
2 being recorded on a computer-readable recording medium.

1 41. A computer-readable recording medium that includes (i)  
2 a read-only unrewritable area and a rewritable area to and from  
3 which data can be written and read, wherein  
4 a medium inherent number inherent to the recording medium  
5 is prestored in the unrewritable area,  
6 a piece of media key data and an encrypted content are  
7 recorded in the rewritable area,  
8 the piece of media key data includes a plurality of  
9 encrypted media keys generated by (i) for each of unrevoked  
10 reproduction apparatuses, encrypting a media key using a device  
11 key of the unrevoked reproduction apparatus respectively, and  
12 (ii) for each of the revoked reproduction apparatuses, encrypting  
13 predetermined detection information using a device key of the  
14 revoked reproduction apparatus respectively,  
15 the encrypted content is generated by encrypting a content  
16 being a piece of digital data, based on an encryption key, and  
17 the encryption key is generated based on the medium  
18 inherent number and the media key recorded in the unrewritable  
19 area of the recording medium.

1 42. A computer-readable recording medium that includes (i)

2 a read-only unrewritable area and a rewritable area to and from  
3 which data can be written and read, wherein  
4 a medium inherent number inherent to the recording medium  
5 is prestored in the unrewritable area,  
6 a piece of media key data and an encrypted content are  
7 recorded in the rewritable area,  
8 the piece of media key data includes a plurality of  
9 encrypted media keys generated by (i) for each of unrevoked  
10 reproduction apparatuses, encrypting a media key using a device  
11 key of the unrevoked reproduction apparatus respectively, and  
12 (ii) for each of the revoked reproduction apparatuses, encrypting  
13 predetermined detection information using a device key of the  
14 revoked reproduction apparatus respectively, and further  
15 includes a data identifier that identifies the piece of media  
16 key data,  
17 the encrypted content is generated by encrypting a content  
18 being a piece of digital data based on an encryption key, and  
19 includes the data identifier, and  
20 the encryption key is generated based on the medium  
21 inherent number and the media key recorded in the unrewritable  
22 area of the recording medium.